(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－144749
（P2001－144749A）
(43)公開日　平成13年５月25日(2001.5.25)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
Ｈ０４Ｌ	9/32		Ｇ０６Ｆ	15/00	３３０Ｂ　５Ｂ０４９
Ｇ０６Ｆ	15/00	３３０	Ｈ０４Ｍ	3/42	Ｔ　５Ｂ０５５
	17/60			11/00	３０２　５Ｂ０８５
	19/00		Ｈ０４Ｌ	9/00	６７３Ｂ　５Ｊ１０４
Ｈ０４Ｍ	3/42		Ｇ０６Ｆ	15/21	３４０Ｂ　５Ｋ０２４

審査請求　未請求　請求項の数６　ＯＬ　（全 10 頁）　最終頁に続く

(21)出願番号　特願平11－321357

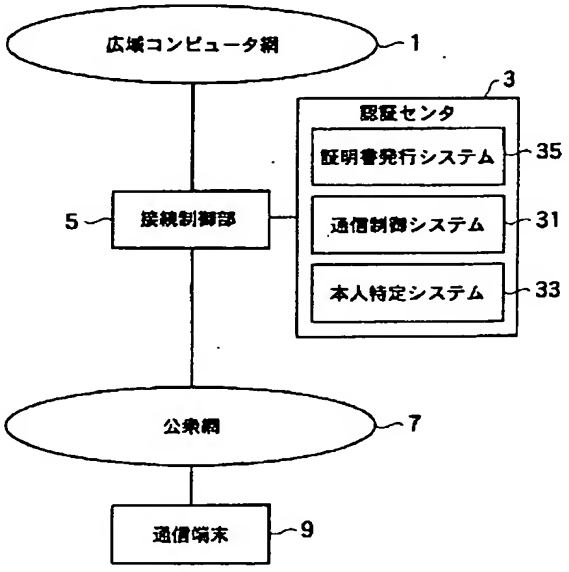
(22)出願日　平成11年11月11日(1999.11.11)

(71)出願人　399041158
西日本電信電話株式会社
大阪府大阪市中央区馬場町３番15号
(72)発明者　吉浦　昭彦
大阪府大阪市中央区馬場町３番15号　西日本電信電話株式会社内
(72)発明者　岩切　高明
大阪府大阪市中央区馬場町３番15号　西日本電信電話株式会社内
(74)代理人　100083806
弁理士　三好　秀和　（外４名）

最終頁に続く

(54)【発明の名称】　ネットワークにおける本人特定方法およびシステムと本人特定プログラムを記録した記録媒体

(57)【要約】
【課題】　本発明は、ネットワークの利用者本人の特定をオンラインで認証することのできるネットワークにおける本人特定方法およびシステムと本人特定プログラムを記録した記録媒体を提供することを目的とする。
【解決手段】　公衆網に接続される通信端末からの電話番号による識別ＩＤを基に与信情報を形成し、該与信情報を出力する電話番号管理手段と、前記公衆網とコンピュータ網との間に設けられ、これら網間の接続を前記与信情報に従って制御する接続制御手段とを備えて構成される。



【特許請求の範囲】
【請求項１】　ネットワーク上における当該ネットワークの利用者本人の特定を当該ネットワークに接続される通信端末からの電話番号により行うことを特徴とするネットワークにおける本人特定方法。
【請求項２】　公衆網に接続される通信端末からの電話番号による識別ＩＤを基に当該公衆網の利用者本人特定のための与信情報を形成し、該与信情報を出力する電話番号管理手段と、
前記公衆網とコンピュータ網との間に設けられ、これら網間の接続を前記与信情報に従って制御する接続制御手段とを有することを特徴とするネットワークにおける本人特定システム。
【請求項３】　前記識別ＩＤは、公衆網から通知される電話番号、または通信端末から通知された電話番号を基にコールバックして確認された電話番号のいずれかであることを特徴とする請求項２に記載のネットワークにおける本人特定システム。
【請求項４】　前記電話番号管理手段は、前記識別ＩＤを基に本人性を判定する本人特定手段と、この本人特定手段からの通知に従って証明書を発行する証明書発行手段とを有することを特徴とする請求項２に記載のネットワークにおける本人特定システム。
【請求項５】　前記電話番号管理手段は、前記識別ＩＤに対応させて少なくとも氏名、住所、カード番号、電子メールアドレスのいずれか１つを格納するデータベースを備えることを特徴とする請求項２または４に記載のネットワークにおける本人特定システム。
【請求項６】　ネットワーク上における当該ネットワークの利用者本人の特定を当該ネットワークに接続される通信端末からの電話番号により行うことを特徴とするネットワークにおける本人特定プログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はネットワーク上の通信相手が現実社会において存在する本人であることを特定することを可能とするネットワークにおける本人特定方法およびシステムと本人特定プログラムを記録した記録媒体に関するものである。
【０００２】
【従来の技術】これまで通信相手を特定するための識別ＩＤとしては、例えばインターネット網ではメールアドレスのように仮想的にコンピュータ網上に設定されたものが用いられており、状況に応じてオフラインで登記簿謄本や戸籍謄本、免許証などの提示を個別に求める場合を除いて、実在する本人をオンラインだけで特定することは困難であり、さらには通信している相手が現実社会上に存在するかどうかについては確実な認証を行うことは行われてはいなかった。
【０００３】また、コンピュータ網と公衆網はまったく異なる通信手順を使用しているため、網上の識別手段も異なり、そのため双方の網に融合性・親和性は乏しく、公衆網は単なる足回りの通信線としてのみ用いられてきた。
【０００４】また、コンピュータ網で情報を安全に通信するために用いらる公開鍵暗号方式では、暗号に使用する鍵と復号に使用する鍵が異なり、通信元は通信相手である通信先の所有する公開された鍵を用いて暗号化し、通信先は自分自身で保有する秘密鍵によって暗号文を復号するようにしている。そのため、通信相手が公開している公開鍵の持ち主が真の通信相手であるということを証明するためのディジタル証明書が必要とされた。
【０００５】
【発明が解決しようとする課題】しかしながら、従来、公開鍵とその持ち主を結び付けるための識別ＩＤとしては、オンラインではメールアドレスのように仮想的に広域コンピュータ網上に設定されたものを用いるしかなかった。そのため、状況に応じてオフラインで登記簿謄本や戸籍謄本、免許証などの提示を求める場合を除いては、実在する鍵の持ち主については、その証明が及ばなかった。すなわち、通信中の情報漏洩・改竄等は暗号通信を採用することにより防ぐことができるものの、通信している相手が現実社会上に存在するかどうかについては証明することはできなかった。
【０００６】また、インターネット網などの広域コンピュータ網へ公衆網を用いて接続する場合には、コンピュータから識別ＩＤとパスワードを入力することにより接続可能なコンピュータユーザであるかどうかを証明するようにしていたため、実在する本人が現実社会に真に存在するかどうかについて確実な認証を行うことは行われなかったし、また行うこともできなかった。
【０００７】本発明は、上記課題に鑑みてなされたもので、ネットワークの利用者本人の特定をオンラインで認証することのできるネットワークにおける本人特定方法およびシステムと本人特定プログラムを記録した記録媒体を提供することを目的とする。
【０００８】
【課題を解決するための手段】前述した目的を達成するために、本発明のうちで請求項１記載の発明は、ネットワーク上における当該ネットワークの利用者本人の特定を当該ネットワークに接続される通信端末からの電話番号により行うことを要旨とする。
【０００９】請求項２記載の発明は、公衆網に接続される通信端末からの電話番号による識別ＩＤを基に当該公衆網の利用者本人特定のための与信情報を形成し、該与信情報を出力する電話番号管理手段と、前記公衆網とコンピュータ網との間に設けられ、これら網間の接続を前記与信情報に従って制御する接続制御手段とを有することを要旨とする。

【００１０】請求項３記載の発明は、前記請求項２記載の識別ＩＤは、公衆網から通知される電話番号、または通信端末から通知された電話番号を基にコールバックして確認された電話番号のいずれかであることを有することを要旨とする。

【００１１】請求項４記載の発明は、前記請求項２記載の電話番号管理手段は、前記識別ＩＤを基に本人性を判定する本人特定手段と、この本人特定手段からの通知に従って証明書を発行する証明書発行手段とを有することを要旨とする。

【００１２】請求項５記載の発明は、前記請求項２または４記載の電話番号管理手段は、前記識別ＩＤに対応させて少なくとも氏名、住所、カード番号、電子メールアドレスのいずれか１つを格納するデータベースを有することを要旨とする。

【００１３】請求項６記載の発明のコンピュータ読み取り可能な記録媒体は、ネットワーク上における当該ネットワークの利用者本人の特定を当該ネットワークに接続される通信端末からの電話番号により行うことを特徴とするネットワークにおける本人特定プログラムを記録したことを要旨とする。

【００１４】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【００１５】図１は、本発明が適用されるシステムの概略の構成を示すブロック図である。図１において、通信端末９は公衆網７を介して、例えばインターネット等の広域コンピュータ網１と接続される。また公衆網７と広域コンピュータ網１との間には接続制御部５が設けられ、この接続制御部５には認証センタ３が接続される。

【００１６】また、認証センタ３は、公衆網７と広域コンピュータ網１との間の通信制御を接続制御部５を介して行う通信制御システム３１と、公衆網７に接続される通信端末９からの電話番号による識別ＩＤを基に本人性を判定し、本人を特定する本人制御システム３３と、この本人制御システム３３から通知される本人性の照合結果を基に証明書を発行する証明書発行システム３５により構成される。

【００１７】また、接続制御部５は、認証センタ３の通信制御部３１の制御指示に従って広域コンピュータ網１と公衆網７との間の接続を制御する。

【００１８】なお、公衆網７と広域コンピュータ網１を含む回線網によりネットワークが構成され、また公衆網７は電話網を含み、かつパケット交換網等のデータ通信網、ＩＳＤＮを含む網であるものとする。また、通信端末９から入力される電話番号としては、１，２，～，９，０の他、通常のプッシュ型の電話機に配備される＃，＊も適宜、使用することができる。

【００１９】次に、公衆網７を介して広域コンピュータ網１へ接続する場合を例に、本実施形態の動作について説明する。

【００２０】まず、モデムやＴＡ（Ｔｅｒｍｉｎａｌ Ａｄａｐｔｅｒ）等の通信端末９によりダイヤルし、電話回線を経由してネットワークへ接続された、モデム付ホストコンピュータ（あるいはダイヤルアップルータ等の通信制御機器）１５等の接続制御部５へ接続を行う。公衆網７では発信者の電話番号を通話開始前に着信者へ通知するという発信者番号通知サービスにより、接続を受ける側で発信者の電話番号を取得、該電話番号を後述する識別ＩＤとした本人特定情報データベースへ照会をかけ、本人特定認証を行う。

【００２１】なお、このとき、このようにＩＳＤＮサービスや携帯電話サービスの基本サービス、アナログ電話サービスでは付加機能である発信側の電話番号を着信側へ通信開始前に通知する発信者電話番号通知サービスによる公衆網７から通知される電話番号に限らず、通信端末から通知された電話番号を基にコールバックして確認された電話番号を用いても良い。

【００２２】さらに本人特定認証が行われた後、広域コンピュータ網１への接続の許可・拒否を電話通信接続が確立する前に行う。また、ディジタル証明書を発行する場合は認証完了後、証明書発行システム３５へ発信者の電話番号を識別ＩＤとして証明書発行要求を行い、公開鍵のディジタル証明書の発行を受ける。

【００２３】次に、図２を参照して、本システムの構成を詳細に説明する。図２において、通信端末としてのモデム付コンピュータ１９は公衆網７を介して、広域コンピュータ網１と接続される。また公衆網７と広域コンピュータ網１との間には、接続制御部としてのモデム付ホストコンピュータ（あるいはダイヤルアップルータ等の通信制御機器）１５が設けられ、このモデム付ホストコンピュータ１５には認証センタ１３が接続される。なお、公衆網７には任意の通信端末が適宜、複数接続される。

【００２４】また、図２に示す公衆網一広域コンピュータ網通信制御システム１３１、本人制御システム１３３およびディジタル証明書発行システム１３５は、図１に示す通信制御システム３１、本人制御システム３３および証明書発行システム３５にそれぞれ対応するものであって、認証センタ１３内に設けられる。

【００２５】公衆網一広域コンピュータ網通信制御システム１３１は、公衆網７と広域コンピュータ網１との間の通信制御をモデム付ホストコンピュータ１５を介して行う。また、本人制御システム１３３は、補助プログラム（１），（２），（３），（４），（５）を格納する。これにより本人制御システム１３３は、該補助プログラム（１），～，（５）を実行することにより、公衆網７に接続される通信端末９からの電話番号による識別ＩＤを基に本人性を判定し、本人を特定する。また、これら補助プログラム（１），～，（５）は、トランザク

ション管理システム１３７により取りまとめられる。
【００２６】ディジタル証明書発行システム１３５は、本人制御システム１３３から通知される本人性の照合結果を基に後述する図８に示すような与信情報としてのディジタル証明書を発行する。
【００２７】さらに認証センタ３内には、データベース１３９が設けられ、このデータベース１３９には、電話番号による識別ＩＤデータ１３９ａ、本人特定データ１３９ｂ、識別ＩＤ変換データ１３９ｃが格納される。
【００２８】識別ＩＤデータ１３９ａは電話番号によるデータであり、本人特定データ１３９ｂは着呼側の着信者電話番号に付随して送信される発呼側の発信者電話番号から本人の特定を行うためのデータであり、識別ＩＤ変換データ１３９ｃは電話番号を本人特定問い合わせ先に対応したデータ（例えば口座番号）に変換するためのテーブルを有するデータである。
【００２９】また、モデム付ホストコンピュータ１５には、識別ＩＤ通信バッファリングシステム１５１が設けられる。この識別ＩＤ通信バッファリングシステム１５１は、通信速度一定の公衆網７と通信速度不定の広域コンピュータ網１との間の整合をとるためのバッファである。
【００３０】以下、図３乃至図７を参照して、本実施形態の動作を詳細に説明する。
【００３１】ここではモデム付コンピュータ１９を使用して、公衆網７へアクセスし、広域コンピュータ網１へ接続する場合について説明する。
【００３２】まず、モデム付ホストコンピュータ１５へモデム付コンピュータ１９から電話をかけ、電話通信接続が試行される。公衆網７はモデム付ホストコンピュータ１５に着信が行われる前にモデム付コンピュータ１９が発信に利用した電話回線の電話番号（発信者電話番号）を通知する（ステップＳ１１）。
【００３３】ステップＳ１３では、発信者電話番号が通知されると、モデム付ホストコンピュータ１５が、この通知された発信者電話番号を公衆網－広域コンピュータ網通信制御システム１３１を介して本人特定システム１３３に渡す。本人特定システム１３３は、図３に示す補助プログラム（１）乃至（５）を起動する。
【００３４】補助プログラム（１）おいては、電話番号を識別ＩＤとしてデータベース１３９への問い合わせを行い（ステップＳ１５）、受け取った電話番号を識別ＩＤとして本人特定データ１３９ｂを検索し、合致するデータの有無を確認し、本人特定認証を行う（ステップＳ１７）。その認証結果はデータベース１３９へ保存されると同時に、補助プログラム（２）へ渡される（ステップＳ１９）。
【００３５】図４に示す補助プログラム（２）おいては、この認証結果を補助プログラム（１）から受け取る（ステップＳ２１）と共に付加的な情報（パスワードなど）をモデム付コンピュータ１９から受け取り、データベース１３９へ格納する。これらの情報はこのデータベース１３９へ接続可能な他プログラムおよびシステムから利用しても良い。
【００３６】また広域コンピュータ網１への通信制御を行う場合は、補助プログラム（２）から公衆網－広域コンピュータ網通信制御システム１３１へ認証結果が渡され、ステップＳ２３で本人特定認証成功の場合は、モデム付ホストコンピュータ１５は公衆網７から広域コンピュータ網１への通信を許可しステップＳ２７に進み、認証失敗の場合はステップＳ２５に進み、接続拒否する。
【００３７】一方、ステップＳ２３において、公衆網７から広域コンピュータ網１への通信が許可された場合には、広域コンピュータ網１で利用される識別ＩＤであるアドレス、ホスト名がモデム付ホストコンピュータ１５から付与される。
【００３８】付与されたアドレス、ホスト名等の情報は補助プログラム（２）により電話番号と関連付けられたデータベース１３９に格納される（ステップＳ２９）。
【００３９】これらのデータは図６に示す補助プログラム（４）によって、データベースへ識別ＩＤまたはアドレス・ホスト名で検索が行われ（ステップＳ４３）、変換データがあるときには変換が行われ（ステップＳ４５，～，４９）、広域コンピュータ網１側からの本人特定、広域コンピュータ網１から公衆網７へのコンピュータ通信制御に利用される。
【００４０】広域コンピュータ網１と公衆網７の相互通信には、識別ＩＤ通信バッファリングシステム１５１により通信データがバッファリングされ、広域コンピュータ網１上での帯域が保証されない通信手順の場合に、公衆網７との通信手順の相違を吸収する。
【００４１】特に固定長のデータグラムを分割して送受信を行う場合は図７に示す補助プログラム（５）おいて、電話通信接続を監視して（ステップＳ５１）、バッファリングに加えて一時的な蓄積を行い、電話通信接続の有無にかかわらず固定長データグラムの送達を確保する。
【００４２】また、識別ＩＤをもとにディジタル証明書を発行する場合は補助プログラム（１）から図５に示す補助プログラム（３）へ認証結果と識別ＩＤが渡され（ステップＳ３１）、補助プログラム（３）は識別ＩＤによる本人特定認証に成功している場合には（ステップＳ３３）、ディジタル証明書発行システム１３５へ識別ＩＤをもとに証明書発行要求を行う（ステップＳ３５）。
【００４３】発行されたディジタル証明書の「Ｓｅｒｉａｌ　Ｎｕｍｂｅｒ」もしくは「Ｓｕｂｊｅｃｔ　Ｎａｍｅ」に識別ＩＤの情報が格納され、補助プログラム（３）によってモデム付コンピュータ１９へ送信される（ステップＳ３７）。

【００４４】次に図８を参照して、公開鍵ディジタル証明書の一例を説明する。この図８に示す公開鍵ディジタル証明書は、ＩＴＵ－ＴＸ．５０９で規定されている証明書であり、上から順に「Ｖｅｒｓｉｏｎ　Ｎｕｍｂｅｒ；証明書のバージョン（Ｖ１；，Ｖ２；，Ｖ３；）」「Ｓｅｒｉａｌ　Ｎｕｍｂｅｒ；証明書のシリアル番号」「Ｉｓｓｕｅｒ　Ｎａｍｅ；証明書の発行局の情報」「Ｖａｌｉｄｉｔｙ；証明書の有効期限」「Ｓｕｂｊｅｃｔ　Ｎａｍｅ；証明書が証明するユーザの情報」「Ｐｕｂｌｉｃ　Ｋｅｙ；公開鍵の情報」「Ｅｘｔｅｎｓｉｏｎｓ；拡張領域」「Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ；ディジタル署名（内容改竄チェック用）」が記載される。これらの内で、「Ｓｅｒｉａｌ　Ｎｕｍｂｅｒ」と「Ｓｕｂｊｅｃｔ　Ｎａｍｅ」は、発行局が定める、証明書毎にユニークなものである。

【００４５】すなわち、本実施形態においては、電話番号をＩＤとして証明書を発行する場合に、これら「Ｓｅｒｉａｌ　Ｎｕｍｂｅｒ」と「Ｓｕｂｊｅｃｔ　Ｎａｍｅ」のいずれか、または両方を識別ＩＤ（電話番号）として利用することが可能である。

【００４６】次に、図９および図１０を参照して、本人を特定する必要のあるサービスを利用する際の、電話番号による本人特定をより具体的に説明する。図９は電話番号で本人特定を行う際の認証・与信を説明するための図であり、図１０は同じく電話番号の本人特定データへの変換を説明するための図である。

【００４７】まず、図９を参照するに、利用者のパソコン等の通信端末が、有線または無線によりインターネット網等の広域コンピュータ網１にアクセスする際に、各サービス提供者としての、行政機関・役所、２種通信事業者（ＩＳＰ（Ｉｎｔｅｒｎｅｔ　Ｓｅｒｖｉｃｅ　Ｐｒｏｖｉｄｅｒ）等のいわゆるプロバイダ）、バーチャルショップ、金融関連機関（カード会社、銀行及び郵便局等）のいずれと接続するかが選択される。

【００４８】すなわち、利用者がショッピングを楽しみたいときにはバーチャルショップに、バンキングを行おうとする場合には金融関連機関に、住民情報の閲覧・変更を行おうとする場合には行政機関・役所に、インターネット接続を行おうとする場合にはＩＳＰにそれぞれアクセスする。このときアクセスは全て電話番号で行われる。

【００４９】例えば、認証センタとして機能する電話番号管理センタを通じて広域コンピュータ網１に接続して、バーチャルショップでいわゆるクレジットカードを使用して買い物をした場合、バーチャルショップ、カード会社は電話番号をＩＤとして認証代行サービス機関である電話番号管理センタに対して本人を特定するための認証・与信問い合わせを行う。なお電話番号管理センタとしては、通常は認証代行サービスを提供することが可能なＮＴＴおよびその他の電話事業者が対象となる。

【００５０】次に、図１０を参照するに、電話番号管理センタでは、本人を特定するためのデータである本人特定データと、電話番号による識別ＩＤデータとを対応させてデータベースに蓄積している。この本人特定データとしては、本人の氏名・住所、カード会社毎のカード番号、銀行・郵便局毎の口座番号、免許証の免許証番号、保険証券毎の保険証番号、電子メールアドレス、ＵＲＬ（ホームアドレス）が蓄積されている。

【００５１】入力された電話番号からデータベースに蓄積される本人特定データを参照して、例えば行政機関や役所に対しては免許証番号、保険証番号を、ＩＳＰに対しては電子メールアドレス、ＵＲＬを、バーチャルショップに対しては本人の氏名・住所を、カード会社に対してはカード番号を、銀行に対しては口座番号をそれぞれ通知する。

【００５２】ここでは、電話番号管理センタは、バーチャルショップに対しては本人の氏名・住所、電話番号等の商品の発送に係るデータを、カード会社に対しては買い物をした金額の引き落とし電文やカード番号を通知し、これにより与信する。

【００５３】このような本人特定は本人特定プログラムにより実現され、該プログラムはコンピュータで読み取り可能な記録媒体に記録して広く提供される。

【００５４】以下、本人特定プログラムを具体的に説明する。

【００５５】（１）ディジタル証明書発行システムと公衆網に接続された発信者電話番号を受信することができる着信機器（ダイヤルアップルータまたはモデム付ホストコンピュータ）の間に設置されたコンピュータ上の処理プログラムであって、発信者電話番号を受信することができる着信機器から発信者電話番号を受け取り、その発信者電話番号を識別ＩＤとして本人特定情報データベースへ問い合せ、認証成功・失敗等の一連のトランザクションを制御することを特徴とするプログラムである。

【００５６】（２）ディジタル証明書発行システムと公衆網に接続された発信者電話番号を受信することができる着信機器（ダイヤルアップルータまたはモデム付ホストコンピュータ）の間に設置されたコンピュータ上の処理プログラムであって、発信者電話番号を受信することができる着信機器から発信者電話番号を受け取り、その発信者電話番号を識別ＩＤとしてデータベースへ問い合せ、認証完了後、広域コンピュータ網への接続制御を行うことを特徴とするプログラムである。

【００５７】（３）ディジタル証明書発行システムと公衆網に接続された発信者電話番号を受信することができる着信機器（ダイヤルアップルータまたはモデム付ホストコンピュータ）の間に設置されたコンピュータ上の処理プログラムであって、発信者電話番号を受信することができる着信機器から発信者電話番号を受け取り、その発信者電話番号を識別ＩＤとしてデータベースへ問い合

せ、公開鍵ディジタル証明書発行アプリケーションへ発行要求を行う一連のトランザクションを制御することを特徴とするプログラムである。

【００５８】（４）電話番号をアドレスまたはホスト名と関連付けてデータベースに格納された情報をもとに広域コンピュータ網と公衆網の識別ＩＤ変換を行い、本人特定認証、通信制御を行うことを特徴とするプログラムである。

【００５９】（５）識別ＩＤ変換による広域コンピュータ網と公衆網との通信を監視し、電話接続の有無によって通信データをバッファリングもしくは外部記憶装置へ蓄積を行うことを特徴とするプログラムである。

【００６０】上述してきたように、本実施形態によれば、広域コンピュータ網上、オンラインでの情報通信において実在する現実社会との結びつきが提供され、また通信手順の異なる広域コンピュータ網と公衆網の親和性・融合性を高めることができる。

【００６１】すなわち、広域コンピュータ網でなりすましや通信傍受を防ぐために使用されている公開鍵暗号方式において、通信の主体となる公開鍵の持ち主と公開鍵の結びつきをディジタル証明書によって保証する際に、現実社会に存在するものとして、公開鍵の持ち主を特定することが可能となる。

【００６２】また、強度の高い暗号をかける必要がある通信については、当然のことながら通信相手が現実社会に存在することを認証・証明できなければならないが、そのような場合であっても、ディジタル証明書で証明する公開鍵の持ち主に関する情報について登記簿謄本や免許証などの現実社会で通用する証明書の事前提示を行うことなく、広域コンピュータ網の利便性、即時性を生かしてオンラインで認証・証明を行うことを可能とする。

【００６３】さらに各家庭へ広がる通信上の足回りである公衆網と広域コンピュータ網の融合を高められ情報通信分野の発展に寄与するものである。

【００６４】

【発明の効果】以上説明したように、本発明による方法によれば、広域コンピュータ網上の公開鍵暗号化通信で、公開鍵の持ち主が回線契約者として現実に存在することが認証・証明することが可能となり、信頼性、安全性が不可欠で、重要な内容の通信を行うことができるようになる。また、電話番号を識別ＩＤとして接続を制御することで、公衆網と広域コンピュータ網の融合が容易となる。

【図面の簡単な説明】

【図１】本発明が適用されるシステムの概略の構成を示すブロック図である。

【図２】本発明に係る一実施形態の概略の構成を示すブロック図である。

【図３】補助プログラム（１）における処理手順を説明するフローチャートである。

【図４】補助プログラム（２）における処理手順を説明するフローチャートである。

【図５】補助プログラム（３）における処理手順を説明するフローチャートである。

【図６】補助プログラム（４）における処理手順を説明するフローチャートである。

【図７】補助プログラム（５）における処理手順を説明するフローチャートである。

【図８】公開鍵ディジタル証明書の一例を示す図である。

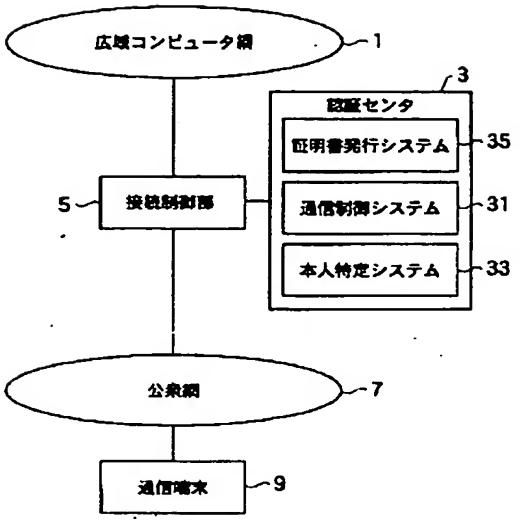
【図９】電話番号で本人特定を行う際の認証・与信を説明するための図である。

【図１０】電話番号で本人特定を行う際の電話番号の本人特定データへの変換を説明するための図である。

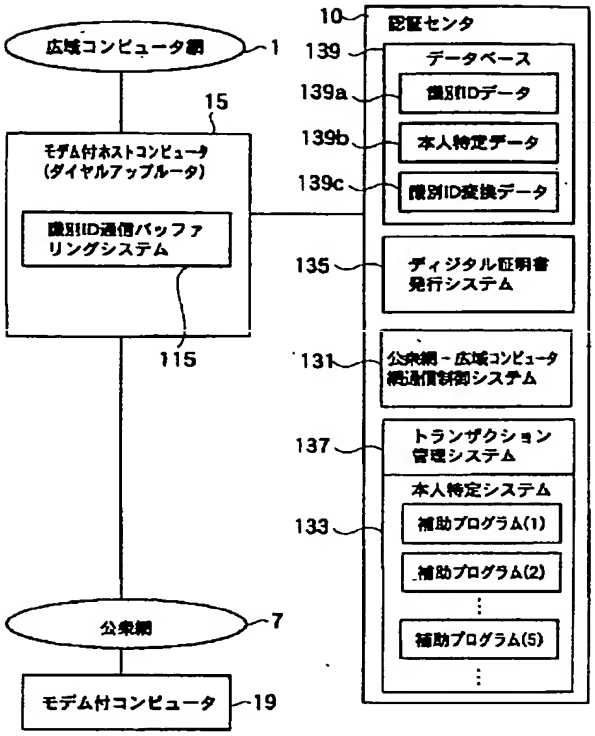
【符号の説明】

１　広域コンピュータ網
３　認証センタ
５　接続制御部
７　公衆網
９　通信端末
１３　認証センタ
１５　モデム付ホストコンピュータ（ダイヤルアップルータ）
１９　モデム付コンピュータ
３１　通信制御システム
３３　本人特定システム
３５　証明書発行システム

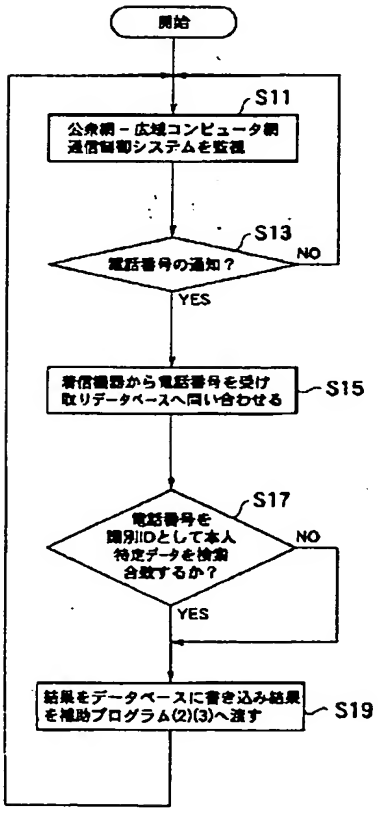
【図1】


広域コンピュータ網
1
3
認証センタ
証明書発行システム
35
接続制御部
5
通信制御システム
31
本人特定システム
33
公衆網
7
通信端末
9

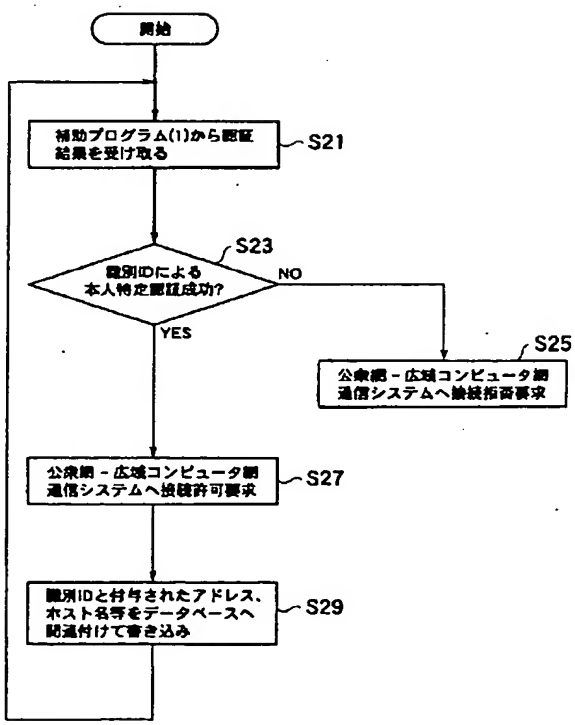
【図2】


10
認証センタ
広域コンピュータ網
1
139
データベース
15
139a
識別IDデータ
モデム付ホストコンピュータ
(ダイヤルアップルータ)
139b
本人特定データ
139c
識別ID変換データ
識別ID通信バッファ
リングシステム
135
ディジタル証明書
発行システム
115
131
公衆網－広域コンピュータ
網通信制御システム
137
トランザクション
管理システム
本人特定システム
133
補助プログラム(1)
補助プログラム(2)
補助プログラム(5)
公衆網
7
モデム付コンピュータ
19

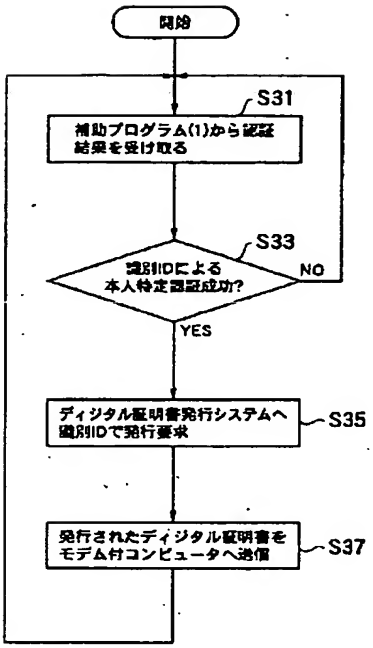
【図3】


開始
S11
公衆網－広域コンピュータ網
通信制御システムを監視
S13
電話番号の通知？
NO
YES
着信端末から電話番号を受け
取りデータベースへ問い合わせる
S15
S17
電話番号を
識別IDとして本人
特定データを検索
合致するか？
NO
YES
結果をデータベースに書き込み結果
を補助プログラム(2)(3)へ渡す
S19

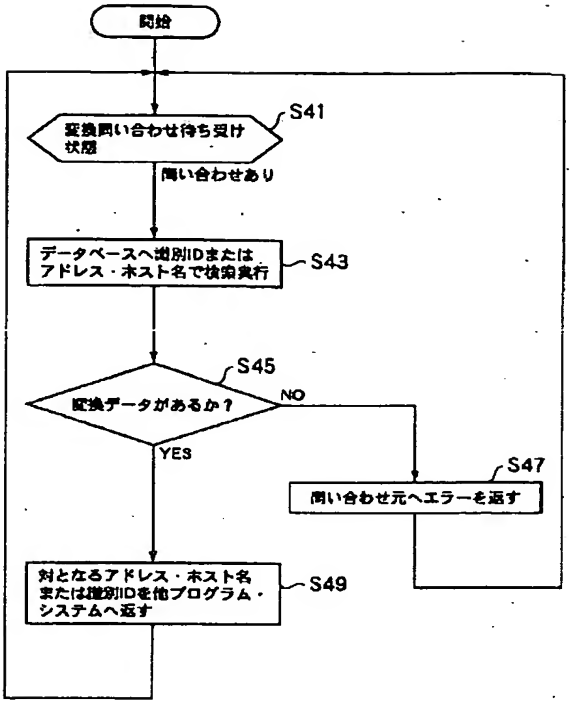
【図4】


開始
補助プログラム(1)から認証
結果を受け取る
S21
S23
識別IDによる
本人特定認証成功?
NO
YES
S25
公衆網－広域コンピュータ網
通信システムへ接続指否要求
公衆網－広域コンピュータ網
通信システムへ接続許可要求
S27
識別IDと付与されたアドレス、
ホスト名等をデータベースへ
関連付けて書き込み
S29

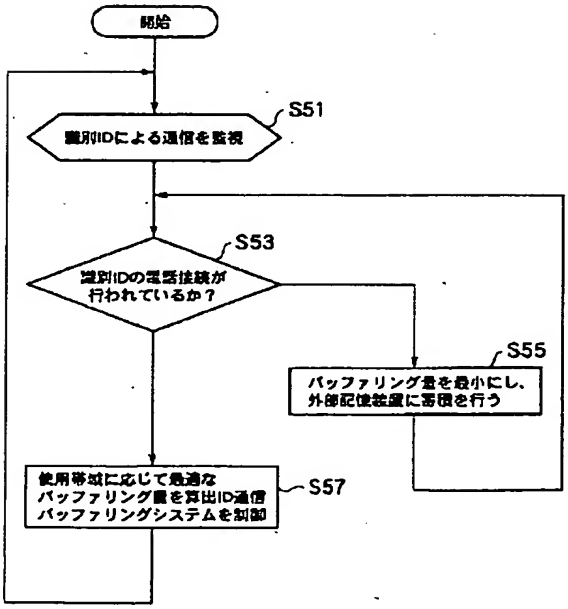
【図5】


開始
S31
補助プログラム(1)から認証結果を受け取る
S33
識別IDによる本人特定認証成功?
NO
YES
ディジタル証明書発行システムへ識別IDで発行要求
S35
発行されたディジタル証明書をモデム付コンピュータへ送信
S37

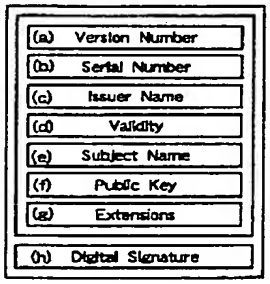
【図6】


開始
S41
変換問い合わせ待ち受け状態
問い合わせあり
データベースへ識別IDまたはアドレス・ホスト名で検索実行
S43
S45
変換データがあるか?
NO
YES
S47
問い合わせ元へエラーを返す
対となるアドレス・ホスト名または識別IDを他プログラム・システムへ返す
S49

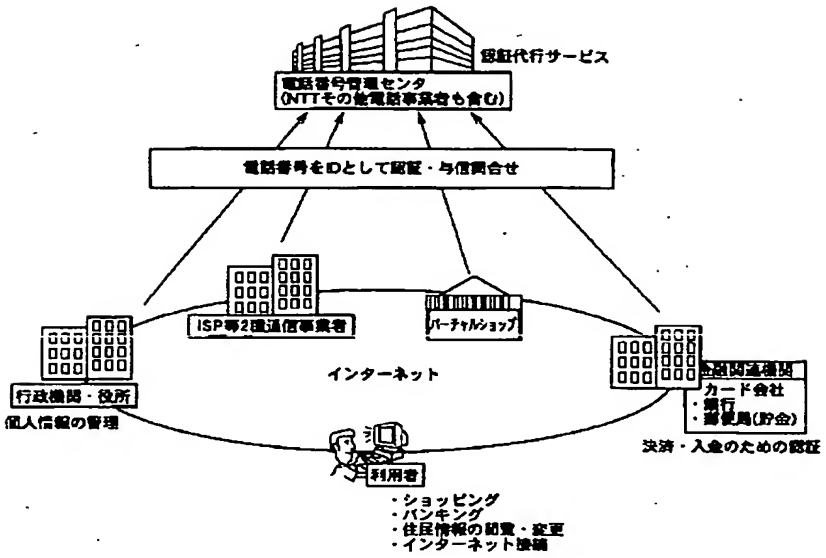
【図7】


開始
S51
識別IDによる通信を監視
S53
識別IDの電子証明が行われているか?
S55
バッファリング量を最小にし、外部記憶装置に書込を行う
使用帯域に応じて最適なバッファリング量を算出ID通信バッファリングシステムを制御
S57

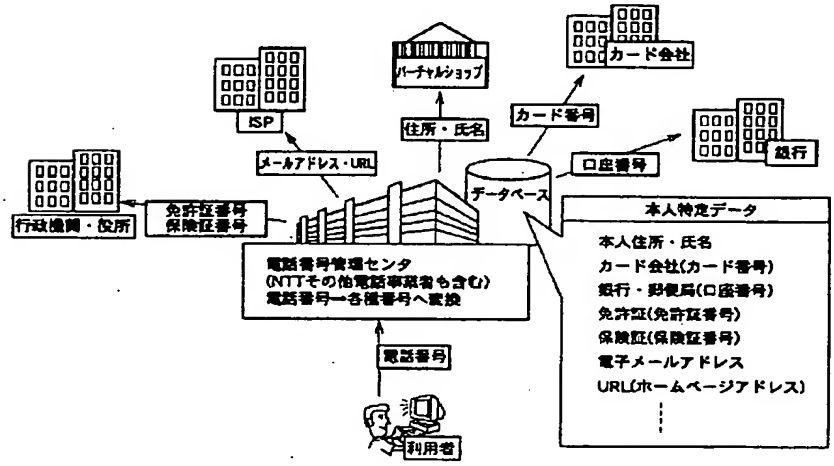
【図8】


(a) Version Number
(b) Serial Number
(c) Issuer Name
(d) Validity
(e) Subject Name
(f) Public Key
(g) Extensions
(h) Digital Signature

【図9】



【図10】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
H04M 11/00	302	G06F 15/30	330	5K101 9A001

(72)発明者 斉川 清二
大阪府大阪市中央区馬場町3番15号 西日本電信電話株式会社内

(72)発明者 黒住 拓弘
大阪府大阪市中央区馬場町3番15号 西日本電信電話株式会社内

(72)発明者　真志喜　卓
大阪府大阪市中央区馬場町３番15号　西日本電信電話株式会社内
(72)発明者　伊吹　元志
大阪府大阪市中央区馬場町３番15号　西日本電信電話株式会社内

Fターム(参考)　5B049 AA05 DD05 EE05 EE09 EE23 EE56 FF09 GG02 GG04 GG07 GG10
5B055 CC10 EE03 EE17 EE21 EE27 HB06 KK01 KK19 PA05 PA34 PA36
5B085 AA08 AE02 AE04 AE09 AE23 BA07 BE07 BG04 BG07
5J104 AA07 BA01 KA01 KA02 NA05 NA27 PA07
5K024 AA62 AA71 AA76 BB04 CC09 DD01 DD04 EE06 FF03 GG01 GG05
5K101 KK16 KK20 LL02 MM04 MM05 MM07 NN03 NN18 NN21 NN25 TT02 UU07 UU16
9A001 BB03 BB04 CC03 DD10 FF03 JJ18 JJ25 KK56 LL03

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-144749
(43)Date of publication of application : 25.05.2001

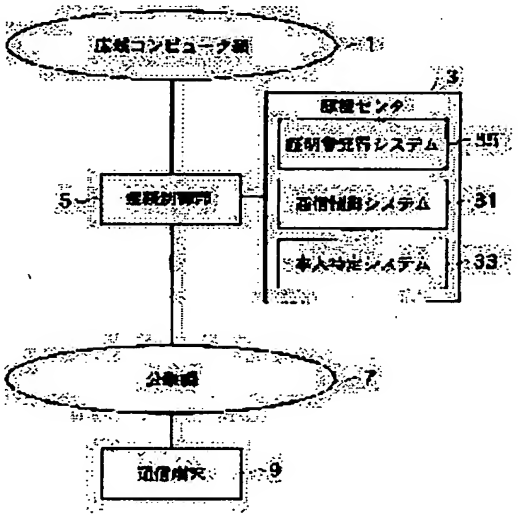
(51)Int.Cl. H04L 9/32
G06F 15/00
G06F 17/60
G06F 19/00
H04M 3/42
H04M 11/00

(21)Application number : 11-321357
(22)Date of filing : 11.11.1999

(71)Applicant : NIPPON TELEGRAPH & TELEPHONE WEST CORP
(72)Inventor : YOSHIURA AKIHIKO
IWAKIRI TAKAAKI
SAIKAWA SEIJI
KUROZUMI TAKUHIRO
MASHIKI TAKU
IBUKI MOTOSHI

(54) METHOD AND SYSTEM FOR SPECIFYING USER CONCERNED AND RECORDING MEDIUM WITH USER SPECIFYING PROGRAM RECORDED THEREON IN NETWORK

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a user specifying method and a device, and a recording medium where a user specifying program is recorded in a network which can authenticate the specification of the network user.
SOLUTION: This system is provided with a telephone number managing means which forms credit information on the basis of an identification ID by a telephones number from a communication terminal connected to a public network and outputs and credit information and a connection control means which is provided between the public network and a computer network and controls connection between the networks according to the credit information.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

* NOTICES *

CLAIMS

[Claim(s)]
[Claim 1] the user of the concerned network on a network — him in the network characterized by performing his specialization by the telephone number from the communication terminal connected to the concerned network — specific technique
[Claim 2] the base [ID / identification / by the telephone number from the communication terminal connected to a public network] — the user of the concerned public network — him in the network characterized by to have a connection control means forms the credit data for he specialization, is established between the telephone number management tool which outputs these credit data, and the aforementioned public network and a computer network, and control the connection between these networks according to the aforementioned credit data — a specific system
[Claim 3] him in the network according to claim 2 characterized by the aforementioned identification ID being either of the telephone numbers checked by calling back on the basis of the telephone number notified from a public network, or the telephone number notified from the communication terminal — a specific system
[Claim 4] the aforementioned telephone number management tool — the base [ID / identification / aforementioned] — him — him who judges a sex — him in the network according to claim 2 characterized by having a specific means and a certificate issue means to publish a certificate according to this notice from a he specialization means — a specific system
[Claim 5] him in the network according to claim 2 or 4 characterized by equipping the aforementioned telephone number management tool with the database which is made to correspond to the aforementioned identification ID and stores any one of a name, the address, a card number, and the e-mail addresses at least — a specific system
[Claim 6] the user of the concerned network on a network — him in the network characterized by performing his specialization by the telephone number from the communication terminal connected to the concerned network — the record medium which recorded the specific program and in which computer reading is possible

[Translation done.]

* NOTICES *

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[The technical field to which invention belongs] him in the network which enables it to specify that this invention is him in whom the communications partner on a network exists in actual society — specific technique and a system, and him — it is related with the record medium which recorded the specific program
[0002]
[Description of the Prior Art] As an identification ID for specifying a communications partner until now For example, what was virtually set as the computer screen oversize like the mail address with the internet network is used. The case where it asks for a presentation of register copy, a copy of a family register, a license, etc., etc. individually off-line according to the status is removed. Performing authentication it being difficult to specify only on-line him who exists really, and positive about whether the partner who is communicating further exists on actual society was not performed.
[0003] Moreover, since the computer network and the public network are using the completely different communication procedure, the identification meanses of a screen oversize also differed, therefore fusion nature and compatibility were deficient in both network, and the public network has been used only as a communication wire of mere axle part.
[0004] Moreover, the key which uses in order to communicate an information safely with a computer network, and is used for an encryption in a **** public key cryptosystem differs from the key used for decode, a communicating agency is enciphered using the exhibited key which the communication place which is a communications partner owns, and the communication place is made to carry out the decode of the cipher with the private key held by himself. Therefore, the digital certificate for the owner of the public key which the communications partner exhibits proving that it is a true communications partner was needed.

[0005]
[Problem(s) to be Solved by the Invention] However, on-line as an identification ID for connecting a public key and its owner conventionally, what was virtually set as the broader-based computer screen oversize like the mail address had to be used. Therefore, if the case where it asked for a presentation of register copy, a copy of a family register, a license, etc., etc. off-line according to the status was removed, the proof did not reach about the owner of the key which exists really. That is, although the information leak, the alteration, etc. under communication could be prevented by adopting cryptocommunication, it was not able to be proved about whether the partner who is communicating exists on actual society.
[0006] Moreover, in connecting with broader-based computer networks, such as an internet network, using a public network, in order to prove whether you are the computer user who can connect by inputting identification ID and a password from a computer, performing authentication positive about whether he who exists really exists in actual society truly was not performed, and it was not able to be performed, either.
[0007] that by which this invention was made in view of the above-mentioned technical

probrem — it is — the user of a network — him in the network which can attest his specialization on-line — specific technique and a system, and him — it aims at offering the record medium which recorded the specific program
[0008]
[Means for Solving the Problem] the user of the concerned network [invention / according to claim 1] on a network in this invention in order to attain the purpose mentioned above — let it be a summary to perform his specialization by the telephone number from the communication terminal connected to the concerned network
[0009] the base [ID / identification / by the telephone number from the communication terminal by which invention according to claim 2 is connected to a public network] — the user of the concerned public network — the credit data for he specialization are formed, and it is prepared between the telephone number management tool which outputs these credit data, and the aforementioned public network and a computer network, and let it be a summary to have a connection control means to control the connection between these networks according to the aforementioned credit data
[0010] Invention according to claim 3 makes it a summary to have that identification ID of the claim 2 aforementioned publication is either of the telephone numbers checked by calling back on the basis of the telephone number notified from a public network, or the telephone number notified from the communication terminal.
[0011] invention according to claim 4 — the telephone number management tool of the claim 2 aforementioned publication — the base [ID / identification / aforementioned] — him — him who judges a sex — let it be a summary to have a specific means and a certificate issue means to publish a certificate according to this notice from a he specialization means
[0012] Invention according to claim 5 makes it a summary to have the database which the aforementioned claim 2 or a telephone number management tool given in four is made to correspond to the aforementioned identification ID, and stores any one of a name, the address, a card number, and the e-mail addresses at least.
[0013] the user of the concerned network [record medium / which invention according to claim 6 can computer read] on a network — him in the network characterized by performing his specialization by the telephone number from the communication terminal connected to the concerned network — let it be a summary to have recorded the specific program
[0014]
[Embodiments of the Invention] Hereafter, the gestalt of operation of this invention is explained using a drawing.
[0015] Drawing 1 is a block diagram showing the configuration of the outline of a system in which this invention is applied. In drawing 1 , a communication terminal 9 is connected with the broader-based computer networks 1, such as internet, through a public network 7. Moreover, the connection control section 5 is formed between a public network 7 and the broader-based computer network 1, and the authentication center 3 is connected to this connection control section 5.
[0016] moreover, on the basis of [the telecommunications control system 31 with which the authentication center 3 performs communications control between a public network 7 and the broader-based computer network 1 through the connection control section 5, and on the basis of identification ID by the telephone number from the communication terminal 9 which connects with a public network 7] — him — him who judges a sex and specifies him — him who is notified from a control system 33 and this he control system 33 — it is constituted by the certificate issue system 35 which publishes a certificate on the basis of a sexual collating result
[0017] Moreover, the connection control section 5 controls the connection between the broader-based computer network 1 and the public network 7 according to control designation of the communications control section 31 of the authentication center 3.
[0018] In addition, a network shall be constituted by the line network containing a public network 7 and the broader-based computer network 1, and a public network 7 shall be a network which contains data communication networks, such as a packet switched network,

and ISDN, including a telephone network. Moreover, as telephone number inputted from a communication terminal 9, # and * which are arranged by the telephone of a usual push type besides 1, 2, −, and 9 and 0 can also be used suitably.
[0019] Next, the case where it connects with the broader−based computer network 1 through a public network 7 is explained to an example about an operation of this operation gestalt.
[0020] First, it dials by the communication terminals 9, such as a modem and TA (Terminal Adapter), and connects with the connection control sections 5, such as the host computer with a modem 15 (or communications control devices, such as a dial−up router) connected to the network via the telephone line. him who set an addresser's telephone number to identification ID which mentions acquisition and this telephone number later by the side which receives connection by the notice service of an addresser number of notifying an addresser's telephone number to an action addressee before telephone call start in a public network 7 — a specific information database — reference — applying — him — specific authentication is performed
[0021] In addition, by the basic service of ISDN service or a cellular−phone service, and the analog call service, you may use the telephone number checked by calling back on the basis of the telephone number notified not only from the telephone number notified from the public network 7 by the caller ID service which notifies the telephone number of the origination side which is an addition function to a destination side before communication start but from the communication terminal in this way at this time.
[0022] Furthermore, after performing he specialization authentication, before [the broader−based computer network 1] telephone communication connection establishes authorization and refusal of connection, it carries out. Moreover, when publishing a digital certificate, a certificate issue demand is performed after the completion of authentication, using an addresser's telephone number as identification ID to the certificate issue system 35, and issue of the digital certificate of a public key is received.
[0023] Next, with reference to drawing 2 , this structure of a system is explained in detail. In drawing 2 , the computer with a modem 19 as a communication terminal is connected with the broader−based computer network 1 through a public network 7. Moreover, between a public network 7 and the broader−based computer network 1, the host computer with a modem 15 as a connection control section (or communications control devices, such as a dial−up router) is formed, and the authentication center 13 is connected to this host computer with a modem 15. In addition, two or more arbitrary communication terminals are suitably connected to a public network 7.
[0024] moreover, the public network−wide area computer network telecommunications control system 131 and him who show in drawing 2 — the telecommunications control system 31 and him who show the control system 133 and the digital certificate issue system 135 in drawing 1 — it is prepared in the authentication center 13 respectively corresponding to the control system 33 and the certificate issue system 35
[0025] The public network−wide area computer network telecommunications control system 131 performs communications control between a public network 7 and the broader−based computer network 1 through the host computer with a modem 15. moreover, him — a control system 133 stores a supplementary program (1), (2), (3), (4), and (5) thereby — him — the base [ID / identification / by the telephone number from the communication terminal 9 connected to a public network 7 when a control system 133 performs this supplementary program (1), −, and (5)] — him — a sex is judged and he is specified Moreover, these supplementary program (1), −, and (5) are adjusted by the transaction managerial system 137.
[0026] the digital certificate issue system 135 — him — him who is notified from a control system 133 — a digital certificate as credit data which is shown in the drawing 8 later mentioned on the basis of a sexual collating result is published
[0027] Furthermore, a database 139 is formed in the authentication center 3, and identification ID data 139a by the telephone number, he specialization data 139b, and identification ID conversion data 139c are stored in this database 139.
[0028] the data for identification ID data 139a being data by the telephone number, and he

specialization data 139b performing his specialization from the addresser telephone number by the side of the call origination transmitted along with the action-addressee telephone number by the side of a call in — it is — identification ID conversion data 139c — the telephone number — him — it is data which have a table for changing into the data (for example, account number) corresponding to the specific reference
[0029] Moreover, the identification ID communication buffering system 151 is formed in the host computer with a modem 15. This identification ID communication buffering system 151 is a buffer for taking matching between the public network 7 of transmission-speed regularity, and the broader-based computer network 1 of a transmission-speed indeterminate.
[0030] Hereafter, with reference to the drawing 3 or the drawing 7 , an operation of this operation gestalt is explained in detail.
[0031] Here, the computer with a modem 19 is used, it accesses to a public network 7, and the case where it connects with the broader-based computer network 1 is explained.
[0032] First, the host computer with a modem 15 is telephoned from the computer with a modem 19, and telephone communication connection is made. A public network 7 notifies the telephone number (addresser telephone number) of the telephone line which the computer with a modem 19 used for dispatch, before performing arrival of the mail to the host computer with a modem 15 (step S11).
[0033] if the addresser telephone number is notified at step S13 — the host computer with a modem 15 — this notified addresser telephone number — the public network-wide area computer network telecommunications control system 131 — minding — him — the specific system 133 is passed The he specialization system 133 starts the supplementary program (1) shown in drawing 3 , or (5).
[0034] the existence of the data which supplementary program (1) set, set the telephone number to identification ID, perform an inquiry in a database 139 (step S15), set the received telephone number to identification ID, search he specialization data 139b, and agree — checking — him — specific authentication is performed (step S17) While the authentication result is saved to a database 139, it is passed to a supplementary program (2) (step S19).
[0035] the supplementary program (2) shown in drawing 4 — setting — this authentication result — a supplementary program (1) **** — receiving (step S21) — additional informations (password etc.) are received from the computer with a modem 19, and it stores in a database 139 It is connectable with this database 139, and also you may use these informations from a program and a system.
[0036] moreover, when performing communications control to the broader-based computer network 1, an authentication result passes the public network-wide area computer network telecommunications control system 131 from a supplementary program (2) — having — step S23 — him — in a specific authentication success, the host computer with a modem 15 permits the communication to the broader-based computer network 1 from a public network 7, it progresses to step S27, and the connection refusal of the case of an authentication failure is progressed and carried out to step S25
[0037] On the other hand, when the communication to the broader-based computer network 1 is permitted from a public network 7 in step S23, the address and the host name which are identification ID used with the broader-based computer network 1 are given from the host computer with a modem 15.
[0038] The given informations, such as the address and a host name, are stored in the database 139 related with the telephone number by the supplementary program (2) (step S29).
[0039] Conversion is performed, when reference is performed by identification ID, or the address and a host name to a database (step S43) and these data have conversion data by the supplementary program (4) shown in drawing 6 (step S4).
[0040] In the two way communication of the broader-based computer network 1 and the public network 7, communication data are buffered by the identification ID communication buffering system 151, and when it is the communication procedure to which the band on the broader-based computer network 1 is not guaranteed, a difference of the communication

procedure with a public network 7 is absorbed.
[0041] When transmitting and receiving by dividing especially the datagram of a fixed length, it supplementary program [which is shown in drawing 7] (5) Sets, and telephone communication connection is supervised (step S51), in addition to buffering, a temporary store is performed, and delivery of fixed-length datagram is secured irrespective of the existence of telephone communication connection.
[0042] moreover, him according [when publishing a digital certificate on the basis of identification ID, an authentication result and identification ID are passed to the supplementary program (3) shown in drawing 5 from a supplementary program (1) (step S31), and / a supplementary program (3)] to identification ID — when having succeeded in specific authentication, a certificate issue demand is performed on the basis of identification ID to (step S33) digital certificate issue system 135 (step S35)
[0043] The information on identification ID is stored in "Serial Number" or "Subject Name" of the published digital certificate, and it is transmitted to the computer with a modem 19 by the supplementary program (3) (step S37).
[0044] Next, an example of a public-key digital certificate is explained with reference to drawing 8 . The public-key digital certificate shown in this drawing 8 is a certificate specified in ITU-T X.509. Version the order from a top "Serial version (V1;, V2;, V3;) of Number; certificate "Issuer serial number of Number; certificate Subject the information on the issue office of Name; certificate", and "the term of validity of Validity; certificate""" "Public an user's information which Name; certificate proves "Digital the information on Key; public key", and "Extensions; extension field" A Signature; digital signature (for a content alteration check)" is indicated." Among these, "Serial Number" and "Subject Name" are unique for every certificate which an issue office defines.
[0045] That is, in this operation gestalt, when publishing a certificate, using the telephone number as ID, it is possible to use these "Serial Number", "Subject Name", or both as an identification ID (telephone number).
[0046] next, him by the telephone number at the time of using the service with the need of specifying him, with reference to the drawing 9 and the drawing 10 — specialization is explained more concretely drawing 9 — the telephone number — him — drawing for explaining the authentication and **** at the time of specifying — it is — drawing 10 — the same — him of the telephone number — it is drawing for explaining conversion to specific data
[0047] First, in case communication terminals, such as a user's personal computer, access the broader-based computer networks 1, such as an internet network, by the cable or the radio with reference to drawing 9 , it is chosen with any of administrative body and public office, two sort communication entrepreneur (so-called **********s, such as ISP (Internet Service Provider)), virtual shop, and financial relation engines (a card issuer, a bank, post office, etc.) it connects. [as each service provider]
[0048] That is, when a user wants to enjoy shopping, a virtual shop is accessed at ISP, respectively, when it is going to perform an Internet connectivity at an administrative body and a public office, when it is going to perform banking and it is going to perform perusal and change of a residents information to a financial relation engine. At this time, all accesses are performed by the telephone number.
[0049] For example, when it connects with the broader-based computer network 1 through the functioning telephone number management center and it buys as an authentication center at a virtual shop using the so-called credit card, a virtual shop and a card issuer perform the authentication and the **** inquiry for specifying him to the telephone number management center which is an authentication vicarious execution service engine, using the telephone number as ID. In addition, NTT as a telephone number management center which can usually offer an authentication vicarious execution service, and other telephone entrepreneurs become an object.
[0050] next, him who is data for specifying him in the telephone number management center with reference to drawing 10 — specific data and the identification ID data by the telephone

number are made to correspond, and it is accumulating in the database As this he specialization data, his name and the address, the card number for every card issuer, the account number for every bank and post office, the license number of a license, the insurance certificate number for every policy, an e-mail address, and URL (home address) are accumulated.

[0051] him who is accumulated from the inputted telephone number at a database — with reference to specific data, the account number is notified [a license number and an insurance certificate number / an e-mail address and URL / his name and the address] for a card number to a bank to a card issuer to a virtual shop to ISP to an administrative body or a public office, respectively

[0052] Here, a telephone number management center notifies the pulling-down wording of a telegram and card number of the amount of money which bought the data applied to dispatch of goods, such as his name and the address, and the telephone number, to a virtual shop to the card issuer, and, thereby, ****s them.

[0053] such him — specialization — him — a specific program is realized, and by computer, this program is recorded on the record medium which can be read, and is offered widely

[0054] the following and him — a specific program is explained concretely

[0055] (1) an arrival-of-the-mail device to the addresser telephone number which is a processing program on the computer installed between the arrival-of-the-mail devices (a dial-up router or host computer with a modem) which can receive the addresser telephone number connected with the digital certificate issue system at the public network, and can receive the addresser telephone number — receiving — the addresser telephone number — an identification ID — carrying out — him — it is the program characterized by to ask a specific-information database and to control a series of transactions, such as an authentication success and a failure

[0056] (2) It is a processing program on the computer installed between the arrival-of-the-mail devices (a dial-up router or host computer with a modem) which can receive the addresser telephone number connected with the digital certificate issue system at the public network, and ask a database, receiving the addresser telephone number from the arrival-of-the-mail device which can receive the addresser telephone number, and using the addresser telephone number as identification ID, and it is the program characterized by to perform the connection control to a broader-based computer network after the completion of authentication.

[0057] (3) It is a processing program on the computer installed between the arrival-of-the-mail devices (a dial-up router or host computer with a modem) which can receive the addresser telephone number connected with the digital certificate issue system at the public network, and it is the program which receives the addresser telephone number from the arrival-of-the-mail device which can receive the addresser telephone number, sets the addresser telephone number to an identification ID, and is characterized by to control a series of transaction which asks a database and performs an issue demand to public-key digital certificate issue application.

[0058] (4) a basis [information / which relates the telephone number with the address or a host name, and was stored in the database] — identification ID conversion of a broader-based computer network and a public network — carrying out — him — they are specific authentication and the program characterized by performing communications control

[0059] (5) It is the program characterized by supervising the communication with the broader-based computer network and public network by identification ID conversion, and accumulating communication data to buffering or external storage by the existence of telephone connection.

[0060] As mentioned above, according to this operation gestalt, the compatibility and the fusion nature of a broader-based computer network and a public network from which the connection with the actual society which exists really in the information communication with a broader-based computer screen oversize and online is offered, and a communication procedure is different can be raised.

[0061] That is, in the public key cryptosystem currently used in order to become, to manage a broader-based computer network and to prevent **********, in case the owner of the public key used as a communicative subject and connection of a public key are guaranteed with a digital certificate, it is enabled to specify the owner of a public key as what exists in actual society.
[0062] moreover, about the communication which needs to apply the encryption with a high intensity Although it must be able to attest and prove that a communications partner exists in actual society with a natural thing, even if it is in such a case It is enabled to perform authentication and proof on-line the convenience of a broader-based computer network, and instancy taking advantage of a sex, without performing a prior presentation of the certificate which is valid in actual society, such as register copy and a license, about the information about the owner of a public key who proves with a digital certificate.
[0063] Fusion of the public network which is the axle part on the communication which furthermore spreads to each home, and a broader-based computer network is raised, and it contributes to development of an information communication field.
[0064]
[Effect of the Invention] According to the technique by this invention, as explained above, by public-key-encryption-ized communication of a broader-based computer screen oversize, it becomes possible [attesting and proving] for the owner of a public key to exist actually as a circuit contractor, and a reliability and safety can be indispensable and can communicate the important content now. Moreover, fusion of a public network and a broader-based computer network becomes easy by controlling connection, using the telephone number as identification ID.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL FIELD

[The technical field to which invention belongs] him in the network which enables it to specify that this invention is him in whom the communications partner on a network exists in actual society — specific technique and a system, and him — it is related with the record medium which recorded the specific program

[Translation done.]

* NOTICES *

PRIOR ART

[Description of the Prior Art] As an identification ID for specifying a communications partner until now For example, what was virtually set as the computer screen oversize like the mail address with the internet network is used. The case where it asks for a presentation of register copy, a copy of a family register, a license, etc., etc. individually off-line according to the status is removed. Performing authentication it being difficult to specify only on-line him who exists really, and positive about whether the partner who is communicating further exists on actual society was not performed.

[0003] Moreover, since the computer network and the public network are using the completely different communication procedure, the identification meanses of a screen oversize also differed, therefore fusion nature and compatibility were deficient in both network, and the public network has been used only as a communication wire of mere axle part.

[0004] Moreover, the key which uses in order to communicate an information safely with a computer network, and is used for an encryption in a **** public key cryptosystem differs from the key used for decode, a communicating agency is enciphered using the exhibited key which the communication place which is a communications partner owns, and the communication place is made to carry out the decode of the cipher with the private key held by himself. Therefore, the digital certificate for the owner of the public key which the communications partner exhibits proving that it is a true communications partner was needed.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

EFFECT OF THE INVENTION

[Effect of the Invention] According to the technique by this invention, as explained above, by public-key-encryption-ized communication of a broader-based computer screen oversize, it becomes possible [attesting and proving] for the owner of a public key to exist actually as a circuit contractor, and a reliability and safety can be indispensable and can communicate the important content now. Moreover, fusion of a public network and a broader-based computer network becomes easy by controlling connection, using the telephone number as identification ID.

[Translation done.]

* NOTICES *

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] However, on-line as an identification ID for connecting a public key and its owner conventionally, what was virtually set as the broader-based computer screen oversize like the mail address had to be used. Therefore, if the case where it asked for a presentation of register copy, a copy of a family register, a license, etc., etc. off-line according to the status was removed, the proof did not reach about the owner of the key which exists really. That is, although the information leak, the alteration, etc. under communication could be prevented by adopting cryptocommunication, it was not able to be proved about whether the partner who is communicating exists on actual society.
[0006] Moreover, in connecting with broader-based computer networks, such as an internet network, using a public network, in order to prove whether you are the computer user who can connect by inputting identification ID and a password from a computer, performing authentication positive about whether he who exists really exists in actual society truly was not performed, and it was not able to be performed, either.
[0007] that by which this invention was made in view of the above-mentioned technical probrem — it is — the user of a network — him in the network which can attest his specialization on-line — specific technique and a system, and him — it aims at offering the record medium which recorded the specific program

[Translation done.]

* NOTICES *

MEANS

[Means for Solving the Problem] the user of the concerned network [invention / according to claim 1] on a network in this invention in order to attain the purpose mentioned above — let it be a summary to perform his specialization by the telephone number from the communication terminal connected to the concerned network
[0009] the base [ID / identification / by the telephone number from the communication terminal by which invention according to claim 2 is connected to a public network] — the user of the concerned public network — the credit data for he specialization are formed, and it is prepared between the telephone number management tool which outputs these credit data, and the aforementioned public network and a computer network, and let it be a summary to have a connection control means to control the connection between these networks according to the aforementioned credit data
[0010] Invention according to claim 3 makes it a summary to have that identification ID of the claim 2 aforementioned publication is either of the telephone numbers checked by calling back on the basis of the telephone number notified from a public network, or the telephone number notified from the communication terminal.
[0011] invention according to claim 4 — the telephone number management tool of the claim 2 aforementioned publication — the base [ID / identification / aforementioned] — him — him who judges a sex — let it be a summary to have a specific means and a certificate issue means to publish a certificate according to this notice from a he specialization means
[0012] Invention according to claim 5 makes it a summary to have the database which the aforementioned claim 2 or a telephone number management tool given in four is made to correspond to the aforementioned identification ID, and stores any one of a name, the address, a card number, and the e-mail addresses at least.
[0013] the user of the concerned network [record medium / which invention according to claim 6 can computer read] on a network — him in the network characterized by performing his specialization by the telephone number from the communication terminal connected to the concerned network — let it be a summary to have recorded the specific program
[0014]
[Embodiments of the Invention] Hereafter, the gestalt of operation of this invention is explained using a drawing.
[0015] Drawing 1 is a block diagram showing the configuration of the outline of a system in which this invention is applied. In drawing 1 , a communication terminal 9 is connected with the broader-based computer networks 1, such as internet, through a public network 7. Moreover, the connection control section 5 is formed between a public network 7 and the broader-based computer network 1, and the authentication center 3 is connected to this connection control section 5.
[0016] moreover, on the basis of [the telecommunications control system 31 with which the authentication center 3 performs communications control between a public network 7 and the broader-based computer network 1 through the connection control section 5, and on the basis of identification ID by the telephone number from the communication terminal 9 which connects with a public network 7] — him — him who judges a sex and specifies him — him who is notified from a control system 33 and this he control system 33 — it is constituted by

the certificate issue system 35 which publishes a certificate on the basis of a sexual collating result

[0017] Moreover, the connection control section 5 controls the connection between the broader-based computer network 1 and the public network 7 according to control designation of the communications control section 31 of the authentication center 3.

[0018] In addition, a network shall be constituted by the line network containing a public network 7 and the broader-based computer network 1, and a public network 7 shall be a network which contains data communication networks, such as a packet switched network, and ISDN, including a telephone network. Moreover, as telephone number inputted from a communication terminal 9, # and * which are arranged by the telephone of a usual push type besides 1, 2, -, and 9 and 0 can also be used suitably.

[0019] Next, the case where it connects with the broader-based computer network 1 through a public network 7 is explained to an example about an operation of this operation gestalt.

[0020] First, it dials by the communication terminals 9, such as a modem and TA (Terminal Adapter), and connects with the connection control sections 5, such as the host computer with a modem 15 (or communications control devices, such as a dial-up router) connected to the network via the telephone line. him who set an addresser's telephone number to identification ID which mentions acquisition and this telephone number later by the side which receives connection by the notice service of an addresser number of notifying an addresser's telephone number to an action addressee before telephone call start in a public network 7 — a specific information database — reference — applying — him — specific authentication is performed

[0021] In addition, by the basic service of ISDN service or a cellular-phone service, and the analog call service, you may use the telephone number checked by calling back on the basis of the telephone number notified not only from the telephone number notified from the public network 7 by the caller ID service which notifies the telephone number of the origination side which is an addition function to a destination side before communication start but from the communication terminal in this way at this time.

[0022] Furthermore, after performing he specialization authentication, before [the broader-based computer network 1] telephone communication connection establishes authorization and refusal of connection, it carries out. Moreover, when publishing a digital certificate, a certificate issue demand is performed after the completion of authentication, using an addresser's telephone number as identification ID to the certificate issue system 35, and issue of the digital certificate of a public key is received.

[0023] Next, with reference to drawing 2 , this structure of a system is explained in detail. In drawing 2 , the computer with a modem 19 as a communication terminal is connected with the broader-based computer network 1 through a public network 7. Moreover, between a public network 7 and the broader-based computer network 1, the host computer with a modem 15 as a connection control section (or communications control devices, such as a dial-up router) is formed, and the authentication center 13 is connected to this host computer with a modem 15. In addition, two or more arbitrary communication terminals are suitably connected to a public network 7.

[0024] moreover, the public network-wide area computer network telecommunications control system 131 and him who show in drawing 2 — the telecommunications control system 31 and him who show the control system 133 and the digital certificate issue system 135 in drawing 1 — it is prepared in the authentication center 13 respectively corresponding to the control system 33 and the certificate issue system 35

[0025] The public network-wide area computer network telecommunications control system 131 performs communications control between a public network 7 and the broader-based computer network 1 through the host computer with a modem 15. moreover, him — a control system 133 stores a supplementary program (1), (2), (3), (4), and (5) thereby — him — the base [ID / identification / by the telephone number from the communication terminal 9 connected to a public network 7 when a control system 133 performs this supplementary program (1), -, and (5)] — him — a sex is judged and he is specified Moreover, these

supplementary program (1), -, and (5) are adjusted by the transaction managerial system 137.
[0026] the digital certificate issue system 135 — him — him who is notified from a control system 133 — a digital certificate as credit data which is shown in the drawing 8 later mentioned on the basis of a sexual collating result is published
[0027] Furthermore, a database 139 is formed in the authentication center 3, and identification ID data 139a by the telephone number, he specialization data 139b, and identification ID conversion data 139c are stored in this database 139.
[0028] the data for identification ID data 139a being data by the telephone number, and he specialization data 139b performing his specialization from the addresser telephone number by the side of the call origination transmitted along with the action-addressee telephone number by the side of a call in — it is — identification ID conversion data 139c — the telephone number — him — it is data which have a table for changing into the data (for example, account number) corresponding to the specific reference
[0029] Moreover, the identification ID communication buffering system 151 is formed in the host computer with a modem 15. This identification ID communication buffering system 151 is a buffer for taking matching between the public network 7 of transmission-speed regularity, and the broader-based computer network 1 of a transmission-speed indeterminate.
[0030] Hereafter, with reference to the drawing 3 or the drawing 7 , an operation of this operation gestalt is explained in detail.
[0031] Here, the computer with a modem 19 is used, it accesses to a public network 7, and the case where it connects with the broader-based computer network 1 is explained.
[0032] First, the host computer with a modem 15 is telephoned from the computer with a modem 19, and telephone communication connection is made. A public network 7 notifies the telephone number (addresser telephone number) of the telephone line which the computer with a modem 19 used for dispatch, before performing arrival of the mail to the host computer with a modem 15 (step S11).
[0033] if the addresser telephone number is notified at step S13 — the host computer with a modem 15 — this notified addresser telephone number — the public network-wide area computer network telecommunications control system 131 — minding — him — the specific system 133 is passed The he specialization system 133 starts the supplementary program (1) shown in drawing 3 , or (5).
[0034] the existence of the data which supplementary program (1) set, set the telephone number to identification ID, perform an inquiry in a database 139 (step S15), set the received telephone number to identification ID, search he specialization data 139b, and agree — checking — him — specific authentication is performed (step S17) While the authentication result is saved to a database 139, it is passed to a supplementary program (2) (step S19).
[0035] the supplementary program (2) shown in drawing 4 — setting — this authentication result — a supplementary program (1) **** — receiving (step S21) — additional informations (password etc.) are received from the computer with a modem 19, and it stores in a database 139 It is connectable with this database 139, and also you may use these informations from a program and a system.
[0036] moreover, when performing communications control to the broader-based computer network 1, an authentication result passes the public network-wide area computer network telecommunications control system 131 from a supplementary program (2) — having — step S23 — him — in a specific authentication success, the host computer with a modem 15 permits the communication to the broader-based computer network 1 from a public network 7, it progresses to step S27, and the connection refusal of the case of an authentication failure is progressed and carried out to step S25
[0037] On the other hand, when the communication to the broader-based computer network 1 is permitted from a public network 7 in step S23, the address and the host name which are identification ID used with the broader-based computer network 1 are given from the host computer with a modem 15.
[0038] The given informations, such as the address and a host name, are stored in the database 139 related with the telephone number by the supplementary program (2) (step

S29).
[0039] Conversion is performed, when reference is performed by identification ID, or the address and a host name to a databasc (step S43) and these data have conversion data by the supplementary program (4) shown in drawing 6 (step S4).
[0040] In the two way communication of the broader-based computer network 1 and the public network 7, communication data are buffered by the identification ID communication buffering system 151, and when it is the communication procedure to which the band on the broader-based computer network 1 is not guaranteed, a difference of the communication procedure with a public network 7 is absorbed.
[0041] When transmitting and receiving by dividing especially the datagram of a fixed length, it supplementary program [which is shown in drawing 7] (5) Sets, and telephone communication connection is supervised (step S51), in addition to buffering, a temporary store is performed, and delivery of fixed-length datagram is secured irrespective of the existence of telephone communication connection.
[0042] moreover, him according [when publishing a digital certificate on the basis of identification ID, an authentication result and identification ID are passed to the supplementary program (3) shown in drawing 5 from a supplementary program (1) (step S31), and / a supplementary program (3)] to identification ID — when having succeeded in specific authentication, a certificate issue demand is performed on the basis of identification ID to (step S33) digital certificate issue system 135 (step S35)
[0043] The information on identification ID is stored in "Serial Number" or "Subject Name" of the published digital certificate, and it is transmitted to the computer with a modem 19 by the supplementary program (3) (step S37).
[0044] Next, an example of a public-key digital certificate is explained with reference to drawing 8 . The public-key digital certificate shown in this drawing 8 is a certificate specified in ITU-T X.509. Version the order from a top "Serial version (V1;, V2;, V3;) of Number; certificate "Issuer serial number of Number; certificate Subject the information on the issue office of Name; certificate", and "the term of validity of Validity; certificate""" "Public an user's information which Name; certificate proves "Digital the information on Key; public key", and "Extensions; extension field" A Signature; digital signature (for a content alteration check)" is indicated." Among these, "Serial Number" and "Subject Name" are unique for every certificate which an issue office defines.
[0045] That is, in this operation gestalt, when publishing a certificate, using the telephone number as ID, it is possible to use these "Serial Number", "Subject Name", or both as an identification ID (telephone number).
[0046] next, him by the telephone number at the time of using the service with the need of specifying him, with reference to the drawing 9 and the drawing 10 — specialization is explained more concretely drawing 9 — the telephone number — him — drawing for explaining the authentication and **** at the time of specifying — it is — drawing 10 — the same — him of the telephone number — it is drawing for explaining conversion to specific data
[0047] First, in case communication terminals, such as a user's personal computer, access the broader-based computer networks 1, such as an internet network, by the cable or the radio with reference to drawing 9 , it is chosen with any of administrative body and public office, two sort communication entrepreneur (so-called **********s, such as ISP (Internet Service Provider)), virtual shop, and financial relation engines (a card issuer, a bank, post office, etc.) it connects. [as each service provider]
[0048] That is, when a user wants to enjoy shopping, a virtual shop is accessed at ISP, respectively, when it is going to perform an Internet connectivity at an administrative body and a public office, when it is going to perform banking and it is going to perform perusal and change of a residents information to a financial relation engine. At this time, all accesses are performed by the telephone number.
[0049] For example, when it connects with the broader-based computer network 1 through the functioning telephone number management center and it buys as an authentication center

at a virtual shop using the so-called credit card, a virtual shop and a card issuer perform the authentication and the **** inquiry for specifying him to the telephone number management center which is an authentication vicarious execution service engine, using the telephone number as ID. In addition, NTT as a telephone number management center which can usually offer an authentication vicarious execution service, and other telephone entrepreneurs become an object.

[0050] next, him who is data for specifying him in the telephone number management center with reference to drawing 10 — specific data and the identification ID data by the telephone number are made to correspond, and it is accumulating in the database As this he specialization data, his name and the address, the card number for every card issuer, the account number for every bank and post office, the license number of a license, the insurance certificate number for every policy, an e-mail address, and URL (home address) are accumulated.

[0051] him who is accumulated from the inputted telephone number at a database — with reference to specific data, the account number is notified [a license number and an insurance certificate number / an e-mail address and URL / his name and the address] for a card number to a bank to a card issuer to a virtual shop to ISP to an administrative body or a public office, respectively

[0052] Here, a telephone number management center notifies the pulling-down wording of a telegram and card number of the amount of money which bought the data applied to dispatch of goods, such as his name and the address, and the telephone number, to a virtual shop to the card issuer, and, thereby, ****s them.

[0053] such him — specialization — him — a specific program is realized, and by computer, this program is recorded on the record medium which can be read, and is offered widely

[0054] the following and him — a specific program is explained concretely

[0055] (1) an arrival-of-the-mail device to the addresser telephone number which is a processing program on the computer installed between the arrival-of-the-mail devices (a dial-up router or host computer with a modem) which can receive the addresser telephone number connected with the digital certificate issue system at the public network, and can receive the addresser telephone number — receiving — the addresser telephone number — an identification ID — carrying out — him — it is the program characterized by to ask a specific-information database and to control a series of transactions, such as an authentication success and a failure

[0056] (2) It is a processing program on the computer installed between the arrival-of-the-mail devices (a dial-up router or host computer with a modem) which can receive the addresser telephone number connected with the digital certificate issue system at the public network, and ask a database, receiving the addresser telephone number from the arrival-of-the-mail device which can receive the addresser telephone number, and using the addresser telephone number as identification ID, and it is the program characterized by to perform the connection control to a broader-based computer network after the completion of authentication.

[0057] (3) It is a processing program on the computer installed between the arrival-of-the-mail devices (a dial-up router or host computer with a modem) which can receive the addresser telephone number connected with the digital certificate issue system at the public network, and it is the program which receives the addresser telephone number from the arrival-of-the-mail device which can receive the addresser telephone number, sets the addresser telephone number to an identification ID, and is characterized by to control a series of transaction which asks a database and performs an issue demand to public-key digital certificate issue application.

[0058] (4) a basis [information / which relates the telephone number with the address or a host name, and was stored in the database] — identification ID conversion of a broader-based computer network and a public network — carrying out — him — they are specific authentication and the program characterized by performing communications control

[0059] (5) It is the program characterized by supervising the communication with the broader-

based computer network and public network by identification ID conversion, and accumulating communication data to buffering or external storage by the existence of telephone connection.

[0060] As mentioned above, according to this operation gestalt, the compatibility and the fusion nature of a broader-based computer network and a public network from which the connection with the actual society which exists really in the information communication with a broader-based computer screen oversize and online is offered, and a communication procedure is different can be raised.

[0061] That is, in the public key cryptosystem currently used in order to become, to manage a broader-based computer network and to prevent **********, in case the owner of the public key used as a communicative subject and connection of a public key are guaranteed with a digital certificate, it is enabled to specify the owner of a public key as what exists in actual society.

[0062] moreover, about the communication which needs to apply the encryption with a high intensity Although it must be able to attest and prove that a communications partner exists in actual society with a natural thing, even if it is in such a case It is enabled to perform authentication and proof on-line the convenience of a broader-based computer network, and instancy taking advantage of a sex, without performing a prior presentation of the certificate which is valid in actual society, such as register copy and a license, about the information about the owner of a public key who proves with a digital certificate.

[0063] Fusion of the public network which is the axle part on the communication which furthermore spreads to each home, and a broader-based computer network is raised, and it contributes to development of an information communication field.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram showing the configuration of the outline of a system in which this invention is applied.
[Drawing 2] It is the block diagram showing the configuration of the outline of the 1 operation gestalt concerning this invention.
[Drawing 3] It is a flow chart explaining the procedure in a supplementary program (1).
[Drawing 4] It is a flow chart explaining the procedure in a supplementary program (2).
[Drawing 5] It is a flow chart explaining the procedure in a supplementary program (3).
[Drawing 6] It is a flow chart explaining the procedure in a supplementary program (4).
[Drawing 7] It is a flow chart explaining the procedure in a supplementary program (5).
[Drawing 8] It is drawing showing an example of a public-key digital certificate.
[Drawing 9] the telephone number — him — it is drawing for explaining the authentication and **** at the time of specifying
[Drawing 10] the telephone number — him — him of the telephone number at the time of specifying — it is drawing for explaining conversion to specific data
[Description of Notations]
1 Broader-based Computer Network
3 Authentication Center
5 Connection Control Section
7 Public Network
9 Communication Terminal
13 Authentication Center
15 Host Computer with Modem (Dial-Up Router)
19 Computer with Modem
31 Telecommunications Control System
33 He Specialization System
35 Certificate Issue System

[Translation done.]